Article can be accessed online at http://www.publishingindia.com

A Key Management Technique to Secure Information Sharing of the Nodes within a Cluster of WSN

Md. Habibur Rahman*, Md. Ibrahim Abdullah**

Abstract

The nodes within a cluster of Wireless Sensor Network deployed in adverse areas face the security threats of eavesdropping and capturing. The fundamental issue in wireless sensor network security is to initialise secure communication between sensor nodes by setting up secret keys between communicating nodes. Because of limited hardware capacity, conventional network cryptography is infeasible for sensor network. In this paper a key management technique is proposed for clustered sensor network that uses some cryptographic operation to generate secret keys. This key is updated in response to the message of cluster head or base station. The key update instructions are stored in each sensor nodes before deployed in sensor field. The updated secret key is used to communicate between nodes and cluster head.

Keywords: Sensor Network, Clustering Technique, Key Management, Authentication, Security

Introduction

A Wireless Sensor Network (WSN) is a collection of tiny nodes with sensors, processor, radio transceiver, and power source. Usually nodes are deployed randomly in sensor field. The sensor nodes are economical and capable of performing military and civilian task such as battlefield surveillance, wildlife tracking, healthcare monitoring, and natural disaster monitoring. Owing to the low cost requirement, sensor nodes should compromise on hardware complexity and have limited computation capability, storage capacity, and radio transmission range. Since sensor nodes are usually powered by batteries, limited power supply is another major concern of WSNs. WSN being often deployed in hostile environment faces the challenge of security and the exiting security mechanisms for the traditional networks are not suitable for it (Laskar & Jena, 2015).

WSNs may be organised in a variety of ways (Akkaya & Younis, 2005). Many sensor networks in real scenarios are organised hierarchically to lower the energy consumption of communication overhead (Heinzelman, Chandrakasan & Balakrishnan, 2000; Lindsey & Raghavendra, 2002). Some nodes of this architecture are grouped to form a cluster. In homogeneous hierarchical sensor networks, Cluster Heads (CHs) are chosen from ordinary sensor nodes based on an application specific metric such as energy consumption, communication cost or latency etc. (Patil, 2004). CH processes information and sends to the base station while the others cluster head's member node perform sensing information. Afte specific time interval, new cluster is rebuilt and formed new node as CH to reduce energy overhead. A well-known cluster-based network, LEACH (Heinzelman *et al.*, 2000; Kaur, 2015), rotates CHs among sensor nodes during different cluster rounds. Minimizing energy consumption among sensor nodes and minimizing the opportunity of attack is the advantages of rotating CHs.

Because of deploying homogeneous sensor nodes in deferent and adverse environment without protection, security issue becomes extremely very important as they are vulnerable to different types of malicious attacks (Kaplantzis, 2006). For example, an adversary can easily listen to the traffic information, who can impersonate one of the network nodes or intentionally provide misleading information to others nodes. Similarly, due to limited resource and computation capability security in sensor network poses different challenges than network security.

* Department of Computer Science and Engineering, Islamic University, Kushtia, Bangladesh.
Email: habibiucse@gmail.com, ibrahim25si@yahoo.com

One security aspects that provides very critical security service in WSN is key management. Key management is the process in which cryptographic keys are generated, stored, updated, protected, transferred, loaded, used and destroyed. A key management system establishes secure communication among the nodes of a cluster ensuring the property that messages are encrypted and communicating nodes are authenticated (Lec, Victor & Leung, 2007).

A key management technique for hierarchically organised wireless sensor network is proposed here to diminish the security concern. The proposed key management technique generates key and update key periodically using mathematical operation which is selected by random number generated by CH or special packet broadcasted by Base Station (BS). All nodes of the network periodically updated their pre-deployed keys to assure that only legitimate nodes will send data for processing.

The rest of the paper is organised as follows: second section describes the related work of security for WSN. Terms and notations used in this paper are listed in third section. Fourth section explains the network model used in this work. Some assumptions about security are described in fifth section. The proposed key management technique is explained in details in the sixth section. Seventh section analyses the proposed method and its limitations. Finally conclusions and future plan is presented in eighth section.

Related Work

Various approaches of key management technique have been discussed in this section. Karlof and Wagner (2003) discuss various attacks and threats of sensor networks against different layers of architecture because of their inherent resource and computing constraints. PKB based broadcast authentication model proposed by Yongshegliu (2011) is used for authentication and has advantages to reduce the overhead in signature amortisation but does not recover the key if it is lost. Owing to cost factor, public key cryptosystems are impractical. Watro, Kong, Cuti, Gardiner, Lynn and Kruus (2004) explain RSA based cryptograph which is applied to wireless sensor network of MICA2 node (MICA2: Crossbow Technologies, 2009). A model of random key pre-distribution scheme for key storage and distribution is being conducted in the research by Du, Deng, Han, Chen and Varshney (2004).

A model of multipath key establishment in paper by Wu and Stinson (2011) proposes technique to enable two nodes to establish secure communication even if they do not share a common key. It also has ability to capture the active attacks but limitation in communication complexity. Eschenauer and Gligor (2002) proposed a random key pre-distribution scheme based on probabilistic key to establish a secure channel. Before the network deployment, each node is assigned to a certain size keys randomly selected from a pre-generated keys pool as its key chain. It also ensures that there is at least a sharing key between two nodes and they can establish direct communication key. This model needs not base station as a communication bridge between any two nodes to establish communication key.

Deployment knowledge based scheme (Du *et al*., 2004), sensor position is known prior to deployment. On account of randomness of deploying nodes it is not possible to know the exact neighbour's locations but knowing the set of likely neighbours is very realistic. Perrig, Szewezyk, Tygar, Wen and Culler (2002) introduced trusted server based solutions is SPINS consisting of Secure Network Encryption Protocol (SNEP) and Micro Timed Efficient Streaming loss-tolerant Authentication protocol (TESLA). SNEP ensures the achievement of communication confidentiality, integrity freshness, and point to point certification. On the other hand, TESLA is used for the point-to-multipoint radio certification.

According to Perrig *et al.* (2002), each node will have a key and corresponding key is stored in the base station whereas a one way hash function is used during the time of broadcast in the authentication to create a release delay mechanism. Only disadvantage of this model is that to establish a direct connection communication key between two nodes is undesirable. A scheme without third party based authority for hierarchical sensor network proposed by Zia & Zomaya (2006a) consists of three keys, two pre-deployed keys in all nodes and one network generated cluster key for a cluster of hierarchical sensor network. This model suggests each node to have mutual authentication with its neighbours and cluster leaders.

Notations used in Proposed Technique

The proposed key management technique uses the following terms and notations:

Table 1: Notation Description

Notation	*Description*
ID	The unique ID of the sensor node
M	Message
K_m	Master Key generated by the base station and pre-deployed in each sensor node and shared by the sensor nodes and base station.
K_i	Secret key generated by the message of cluster head or base station for the node *i* in a cluster.
MAC_{Ki} (M)	Message authentication code for message *M* generated using key K_i.
||	Concatenation operator
⊕	Bit wise XOR operator
……	…….

Proposed Network Model

In our proposed technique, hierarchical structure of sensor network is considered and the networks are homogeneous and symmetric. Node position is random in sensor field. Nodes are static i.e. their positions do not change after deployment. There is a Base Station for processing the sensed data.

After nodes deployment, CHs are selected randomly from the network nodes (Heinzelman *et al*., 2000). Some nodes are randomly selected as CH (Karlof & Wagner, 2003). We assume that communication between member nodes and CH will be single hop, but communication between CH and BS may be single or multihop which depends on the distance between CH and BS.

Security Assumption

We consider the following security assumptions (Zia & Zomaya, 2006b; Roosta, Shieh & Sastry, 2006) common to most WSNs security schemes:

(1) The BS is considered trustworthy with unlimited resources and is located in a safe place. It has authentication system for any node in the network, a node member table of all nodes in the network (Diop, 2014).

(2) Before node deployment, all the sensor nodes share an initial master key K_m and a table of mathematical operation. All the information stored in a semi-permanent memory.

(3) Each sensor has a unique ID with enough length. The BS can use sensor *ID* to distinguish between legitimate *IDs* and malicious ones.

(4) We also consider that after deployment of nodes, it cannot be compromised within a minimum time t_m, because in presence of deployment system an adversary is not able to capture any node.

(5) BS has authentication system (Liu & Ning, 2003) for any node in the network.

(6) To capture a node, connect with a computer and extract information from the node needs a minimum time for an adversary is T_{cap} (Hu, Siddiqi & Sankar, 2007).

The Proposed Key Management Technique

In this proposed key management technique, all nodes are deployed with a master key and a table containing a set of mathematical operation that is used to generate a key. The key and table are stored in flash memory that can be erased or modified when BS sends any command or special packet to the nodes. This mathematical operation uses cluster head ID and node ID as its input data. Other values such as some prime number or some random number is inserted in the table as required for the operation.

Cluster Head Member Key Table

Once the clusters are formed and CHs are selected or elected, they create a database of their member nodes *ID* within time T_{min}. Each CH generates a random number *R* that selects any cryptographic operation from a table that is stored before deployment of nodes. All nodes use this table to create a secret key to communicate with CH.

Table 2: Cryptographic Key Generation Table

1	K_i=	Node ID	||	CH ID
2	K_i=	Node ID*CH ID	-	4-bit left shift of CH ID
3	K_i=	Left shift Node ID 4-bit	OR	(CH ID ⊕ 16-bit prime no)
4	K_i=	Inverse Node ID	AND	CH ID
5	K_i=	Right shift Node ID 7-bit	XOR	CH ID
..	..	…	..	…..

The CH construct a message M using this random number *R*. Simply M is the encrypted form of R by using master key K_m.

$$M = K_m(R)$$

Now CH sends M to all its member nodes as follows –

CH ID	M	MAC (M)

where MAC (M) is the Message Authentication Code of M

CH calculates the key of each node as it knows the ID of all nodes and contain the operation table.

Table 3: Cluster Head's Table Consists of Member Node ID and Secret Key

Member ID	*Key*
08	10001001
10	10010101
11	10010100
14	11010110
16	11101100
…	…

Node Secret Key Creation

After receiving the encrypted random number sent by the CH, all member nodes generate the secret key from the table stored in their memory. For example, the member node of the CH generates a key to communicate with their cluster head. If a member node of ID 10 the cluster receives a packet of random number whose value is 4, then the node of ID 10 construct its secret key K_i to encrypt the data when need to communicate with CH (Table 2).

$$K_i = (\text{Inverse Node ID}_i) \text{ AND } (\text{CH ID}_j)$$

When a member node sends data to its cluster head it encrypt the data using the key K_i, and construct its MAC and packet formats to be sent to the cluster head as follows:

$$E_{Ki}(M) = M_E$$

$$MAC = MAC_{Ki}(M)$$

Packet format become as

ID_i	CH_j	M_E	MAC

The CH knows its all member node ID and also know how to generate key K_i. The CH can easily decrypt the message sent by its member node.

Effects of Clustering Technique

We consider two different scenario of clustering as follows:

1. Cluster head is fixed until its death.
2. Cluster head changed among the sensor nodes.

Fixed CH

In this case, the CH generates a random number *R* after a predefined time interval. After that time interval, the CH broadcasts this random number *R* to its member node in encrypted form using master key K_m. CH construct a new key table. The key table of CH contains the secret keys of its member nodes. After receiving the random number in its encrypted form, the member nodes discards the previous key K_m and updates their key with the received random number to communicate with the CH.

Cluster Head Changed among the Sensor Nodes

We consider that CH changed among the sensor nodes to balance the energy consumption. In this case, after every fixed time interval, cluster is reconstructed. In that case, base station broadcast a special packet to all nodes in the sensor field. All cluster head erase its member key table. When clusters are rebuilt, all clusters create its cluster's member key table as described earlier. As discussed in previous section, CH generates random number *R* after a predefined time interval. CH broadcasts this random number *R* to its member nodes, generates key tables. Member nodes discard the previous key K_m and update their key with the received random number to communicate with the CH.

Sensor Death

When a node's available power drops below a certain level, node sends a Node Death message to its CH. CH removes this node from its cluster member table and broadcasts a notification to its cluster members and BS. This message instructs all nodes in the cluster to remove that node from their neighbor tables.

Proposed key management techniques can be sum up in two parts – for cluster head and member nodes.

Cluster Head Algorithms

The cluster head algorithms perform the following functions

Step 1: Cluster head generates random number R.

Step 2: It sends random number R to all its member nodes.

Step 3: Cluster head creates secret key table as it knows all ID's of its members.

Step 4: If cluster head needs to communicate with node *i*, it constructs a message M, encrypted using K_i, calculate MAC using K_m and send it to node i.

Step 5: Cluster head checks time, if time is expired; cluster head generates random numbers R again and broadcast this to its member nodes to update keys.

Step 6: It update member nodes keys table.

Member Node Algorithm

The node algorithm performs the following functions:

Step 1: Sensor Node requires CH's packet to select an operation.

Step 2: Upon received CH's packet, sensor node performs the operations and finally generate secret key K_i

Step 3: When Sensor Node needs to send data, sensor node encrypt the data using key K_i and constructs its MAC and packet format and send it to the cluster head.

Step 4: If sensor node receives any message of R, it updates the key K_i as per instruction in the table of operation

Step 5: Sensor node then sends data to the cluster head encrypted with new generated secret key.

Security Analysis

The proposed key management technique is analysed in this section. Security depth of our proposed key management scheme depends on the length of key, secret key generation mathematical operation, and time interval of periodically broadcasting random number. CH sends key message in encrypted form to other member nodes so that it is not possible for an eavesdropper to guess any information about the key. After the cluster formation phase, the cluster head's member key is calculated using the random number generated by cluster head as the cluster head knows the master key and ID of each node of its cluster. This key is updated in regular interval when cluster head send message to select an operation of the stored table. So it is not possible for an eavesdropper to extract key from a transmitted message. For a Brute-force attack, if the key is 56 bits long, then there are 2^{56} possible keys and for 64 bits key there are 2^{64} possible keys. An adversary with cost of $100 Million at 1995, he takes 2 minutes for 56 bit key, 9 hours for 64-bit and 70 years for 80-bit key (Schneier, 1996).

Another possible attack is node capturing. This attack can be minimised if cluster head periodically generates and broadcasts a random number to select a table of mathematical operation before minimum time of node capture T_{cap} to update the key. An adversary fails to update the key K_i if the node of a cluster is not captured within node capturing time. CH cannot decrypt the message from a node or BS failed to decrypt the message from a CH, it can be decided that this node is compromised and reject all data from that node. Because of rotating CH among the nodes, if a cluster head is compromised, it will not able to send false data to BS for a long time and after specific time interval a new cluster is rebuilt. Then, adversary needs to capture new CH.

Applying LEACH protocol without any addition provides us with some level of security. This level of security gives WSN the ability to defeat several kinds of insider attacks (Abuhelaleh, 2010).

Limitation of this proposed technique is that if a node is not able to update its secret key on account of communication problems, it assumes the node as malicious node to the network. To avoid this, we need explicit authentication technique from CH to that node. Another limitation is that of frequently receiving packet of random number from CH which increases the overhead of energy. On the other hand, cluster head energy drained due to frequent transmission of packet.

Conclusion

Our proposed key management technique is used to secure communication by generating and updating secret key at regular interval and to mitigate the matter of node

capturing. In proposed technique, base station divides the sensor nodes into cluster and periodically rebuilds the cluster. There is no matter of how many sensor nodes and how many clusters are in a WSN and the nodes can establish the secret key. Therefore, this technique is especially adoptable for inherent resource and computing constrained large scale WSNs. In our proposed key management technique, memory required for storing the key information is acceptable for present hardware of nodes. The nodes communication overhead to exchange the secret key is also minimum. Our future works is to analyze the cost of energy of this technique and introduce a key-recovering technique when a legitimate node failed to update its key due to communication disturbance.

References

Abuhelaleh, M A. (2010). Security in wireless sensor networks: Key management module in SOOAWSN. *International Journal of Network Security & Its Applications*, October, 2(4), 67-78.

Akkaya, K., & Younis, M. (2005). A survey of routing protocols in wireless sensor networks. *Ad Hoc Network Journal*, 3(3), 325-349.

Diop, A. (2014). An improved key management scheme for hierarchical wireless sensors networks. *Indonesian Journal of Electrical Engineering*, May, 12(5), 3969-3978.

Du, W., Deng, J., Han, Y., Chen, S., & Varshney, P. (2004). *A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge*. In IEEE INFOCOM.

Eschenaur, L., & Gligor, V. D. (2002). *A Key Management Scheme for Distributed Sensors Networks*. In Proceedings of the 9th ACM Conference on Computer and Communications Security, (pp. 41-47). Washington, DC, USA: ACM Press.

Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). *Energy Efficient Communication Protocol for Wireless Micro-sensor Networks*. In Proceedings of the 33rd Hawaii International Conference on System Sciences.

Hu, F., Siddiqi, W., & Sankar, K. (2007). *Scalable security in Wireless Sensor and Actuator Networks (WSANs): Integration re-keying with routing*. Computer Networks, 51, 285-308, Science Direct, Elsevier.

Kaplantzis, S. (2006). Security Models for Wireless Sensor Networks.

Karlof, C., & Wagner, D. (2003). Secure routing in sensor networks: Attacks and countermeasures. *Ad Hoc Networks Journal*, 1(2-3), 293-315.

Kaur, G. (2015). Survey on various key management Schemes for LEACH in wireless sensor networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, March, 5(3), 205-209.

Laskar, T., & Jena, D. (2015). A secure key management scheme for hierarchical WSN. *Computer Engineering and Intelligent Systems*, 6(2), 30-36.

Lec, J. C., Victor, C., & Leung, M. (2007). *Key Management Issues in Wireless Sensor Networks: Current Proposals and Future Developments*. In Proceeding of IEEE Wireless Communications, (pp. 76-78).

Lindsey, S., & Raghavendra, C. S. (2002). *PEGASIS: Power Efficient Gathering in Sensor Information Systems*. In the Proceedings of the IEEE Aerospace Conference, Big Sky, Montana.

Liu, D., & Ning, P. (2003). *Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks*. In Proceedings of the 10th Annual Network and Distributed System Security Symposium, (pp. 263-276), San Diego, California, February.

MICA2: Crossbow Technologies. (2009). Retrieved from www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf

Patil, S. (2004). *Performance Measurement of Ad Hoc Sensor Networks Under Threats*. In IEEE Communications Society, Wireless Communications and Networking Conference (WCNC), Atlanta, USA.

Perrig, A., Szewezyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networking*, 8(5), 521-534.

Roosta, T., Shieh, S., & Sastry, S. (2006). *Taxonomy of security attacks in sensor networks and counter-measures*. Berkeley, California, University Press, 2006.

Schneier, B. (1996). *Applied cryptography*. John Wiley & Sons (2nded).

Watro, R., Kong, D., Cuti, S. Gardiner, C., Lynn, C., & Kruus, P. (2004). *Tinypk: Securing Sensor Networks with Public Key Technology*. In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), pp. 59-64.

Wu, J., & Stinson, D. R. (2011). Three *Improved Algorithms for Multipath Key Establishment in Sensor Networks Using Protocols for Secure Message Transmission.*

In Proceeding of IEEE Transaction on Dependable and Secure Computing, November/December, 8(6), 785-797.

Yongshegliu. (2011). *PKC Based Broadcast Authentication using Signature Amortization for WSNs*. In Proceeding of IEEE Transaction on Wireless Communications, June, 11(6), 581-587.

Zia, T. A., & Zomaya, A. Y. (2006a). *Security Issues in Wireless Sensor Networks*. In the Proceedings of the International Conference on Systems and Networks (ICSNC'06), November, (pp. 2-4). Tahiti, French Polynesia.

Zia, T. A., & Zomaya, A. Y. (2006b). *A Security Framework for Wireless Sensor Networks*. In Proceedings of the IEEE Sensor Applications Symposium SAS, February, pp. 7-9, Houston, Texas, USA.